FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1217765-0

Total Deleted Page(s) = 4
Page 20 ~ b7E;
Page 21 ~ b7E;
Page 22 ~ b7E;
Page 25 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

Counterintelligence:
Safeguarding Your Technology

SSA [redacted]

b6
b7C

FBI Priorities

To protect the United States . . .

From terrorist attack

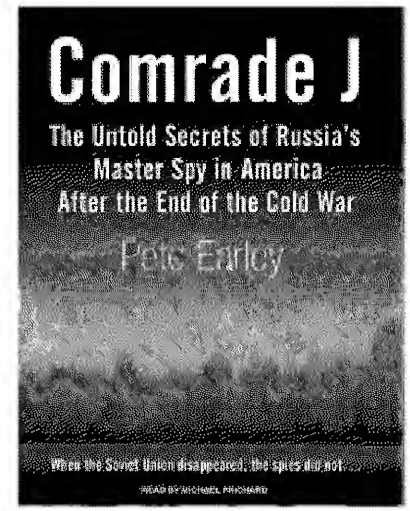
Against foreign intelligence operations/espionage

Against cyber-based attacks and high tech crimes

FBI Director Robert S. Mueller III
June 21, 2002
Congressional Testimony

Counterintelligence Threat

- The symmetric threat still exists, though the asymmetric threat has become more prevalent.
- Foreign adversaries are using every means available to acquire information and technology to gain political, military and economic advantage over the U.S.
- They leverage the placement and access of nearly every profession and every "walk of life" to achieve their objectives.
- Global cyber environment provides non-traditional ways for foreign adversaries to remotely surveil, target, acquire and or exploit our information without setting foot on U.S. soil.



3 Generals

Loss or compromise of U.S Technology

- Classified/National Security Defense Information (Espionage)
- Dual–Use & ITAR Export Restricted Technologies (Export Compliance)
- Sensitive but Unclassified Technologies (IPR)

MEDIA REPORTS ON ECONOMIC ESPIONAGE
PRESS CONFERENCE AND REPORT

U.S. Report Accuses China, Russia of Cyber Attack
Statement by Robert "Bear" Bryant, National Counterintelligence Executive, upon the release of "The Report to Congress on Foreign Economic Collection and Industrial Espionage."

WALL STREET JOURNAL

China Singled Out for Cyber Spying
The U.S. government accused the Chinese of being the world's "most active and persistent" perpetrators of economic spying, an unusual move designed to spur stronger U.S. and international action to combat rampant industrial espionage threatening U.S. economic growth.

CNN

Report: Russia and China are Top Thieves of U.S. Technology
For the first time, the United States is publicly accusing China and Russia of being the top offenders in the theft of U.S. economic and technology information.

The Washington Post

In a World of Cybertheft, U.S. names China, Russia as Main Culprits
Online industrial spying presents a growing threat to the U.S. economy and national security. China and Russia are accused of responsibility of cyber-espionage.

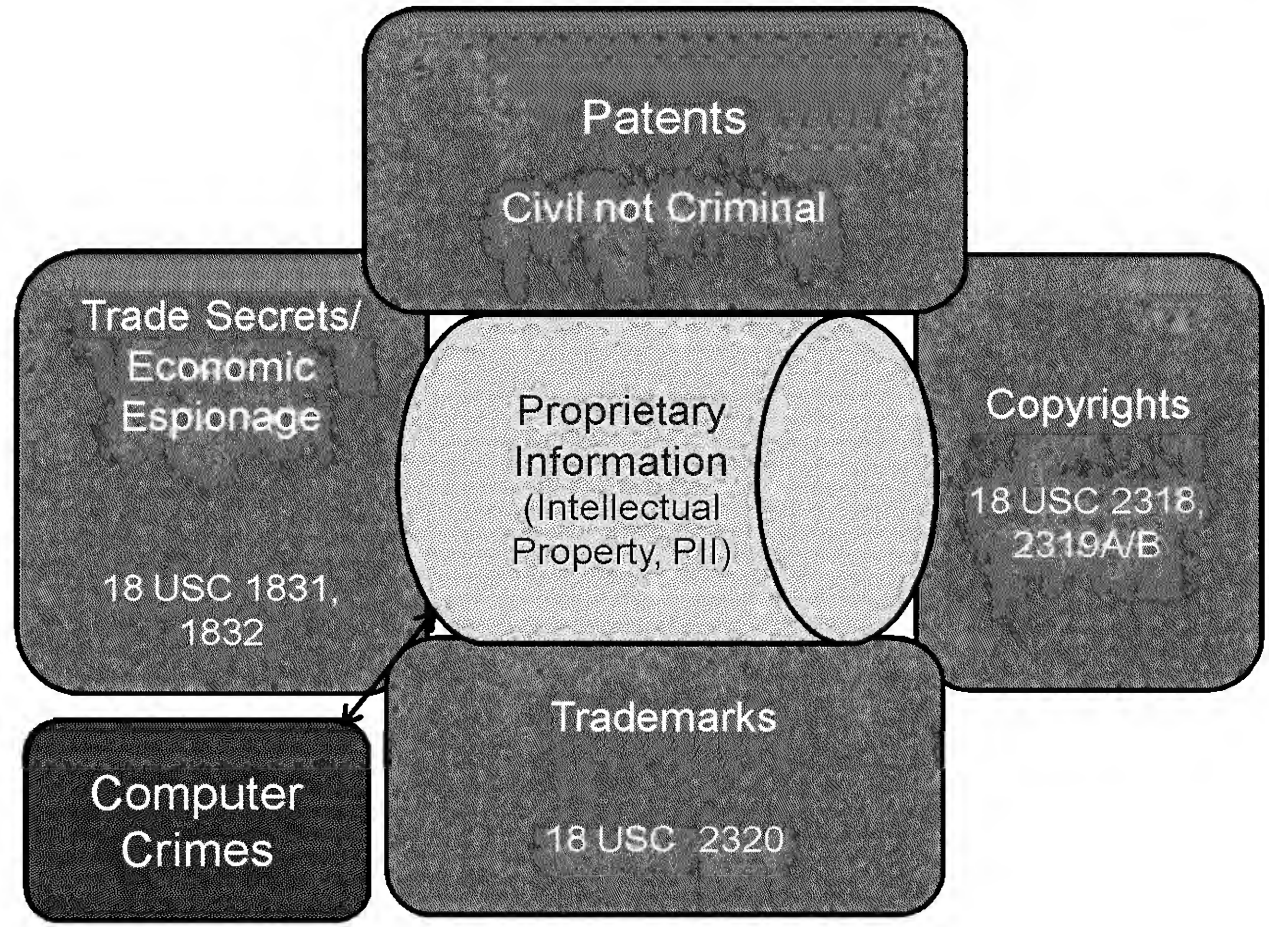
npr
npr.org

China, Russia Top List Of U.S. Economic Cyber Spies
China and Russia have been named as the top culprits in the theft of U.S. intellectual property and technology. This theft is eroding the U.S. global economic advantage, which has long been based on technological innovation.

The Washington Times

US report blasts China, Russia for cybercrime
U.S. intelligence officials accused China and Russia on Thursday of systematically stealing American high-tech data for their own national economic gain.

Types of Unclassified Sensitive/Critical Information



Loss of Corporate IP

How does IP get lost?

- 52% from former employees
- 92% from employees in a non-malicious manner
- 59% from exiting employees
- 25% remaining employees

-From a survey of Fortune 500 companies

Economic Espionage Act of 1996

- Theft of Trade Secrets
  - Title 18, USC Section 1831-1839

- Section 1831
  - Punishes the theft of trade secrets to benefit a foreign government, instrumentality, or agent.

- Section 1832
  - Punishes the commercial theft of trade secrets carried out for economic advantage, whether or not it benefits a foreign government.

  - Territorial Limits
    EEA protects against theft that occurs either (1) inside the U.S., or (2) outside the U.S. and (3) an act in furtherance of the offense was committed in the U.S. or (4) the violator is a U.S. person or organization.

EEA (cont'd)

- EEA was not intended to punish employees who move from one job to another based on their general knowledge
- EEA was not intended to punish competition, even when such competition relies on the know-how of former employees
- EEA was intended to prevent those employees (or their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere.

18 U.S.C. Section 1831 economic espionage

a) Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly –

1. steals, or without authorization copies, duplicates, takes, carries away or conceals, or by fraud, artifice, or deception obtains a trade secret:

2. without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mail, communicates, or conveys such information:

18 U.S.C. Section 1831 economic espionage

3. receives, buys, possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization

4. Attempts to commit paragraph 1-4

5. Conspiracy with more then one person to commit any offense of paragraph 1-4

Penalty: For an individual, not more than 15 years and/or $500,000 fine;

For an organization, a fine of not more than $10,000,000.

18 U.S.C. 1832 theft of trade secrets

a) Whoever, with the intent to convert a trade secret, that is related to or included in a product that is owned produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other then the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly –

1. steals, or without authorization copies, duplicates, takes carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret:

2. without authorization copies, duplicates, sketches, draw, photographs, downloads, uploads, alters, destroys, photographs, replicates, transmits, delivers, send, mails, communicates, or conveys such information:

18 U.S.C. 1832 theft of trade secrets

3. receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

4. attempts to commit any offense described in any paragraphs (1) through (3);

5. Conspires with one or more persons to commit any offense described…

Penalty: For an individual, imprisonment for not more than 10 years; no fine limit stated in the statue. For an organization, a fine of not more than $5,000,000

Trade Secret Examples

- What types of things can be trade secrets? (Section 1839)
  - Manufacturing processes
  - Financial Information
  - Lists of Suppliers/Customers
  - Computer Source Code
  - Chemical Formulas
  - Marketing Strategies
  - Research & Development Data
  - Engineering plans and compliations

Caveats: (1) Owner has taken reasonable measures to protect and (2) has an independent economic value.

Who has been targeted?

Goldman Sachs

CARGILL

MOTOROLA

Cleveland Clinic

Coca-Cola classic

L3 communications

DOW

valspar

BOEING

Sun microsystems

DUPONT

NORTHROP GRUMMAN

GOODYEAR

PPG

GM

Ford

Bristol-Myers Squibb

AVERY DENNISON

ST. JUDE MEDICAL
MORE CONTROL. LESS RISK.

Proactive Measures

- Report suspicious activities quickly (Insider Threat/Cyber Intrusions).
- Recognize that countries may target your technology and research.
- Understand military or dual uses.
- Prevent unnecessary access.
- Be cautious in responding to requests for information.
- Implement a definable plan for safeguarding intellectual property.

Proactive Measures

- Secure physical trade secrets and limit access to trade secrets.
- Confine intellectual knowledge.
- Provide ongoing security training to employees.

Policy Considerations

- Is it documented that an employee has the authority to have a home office?
- Are employees allowed access to IP after giving two weeks notice?
- Is there company policy regarding proper markings on documents, E-Mails, etc with IP, i.e. Confidential?
- Are employees trained on handling and storage of IP?
  - Is the training documented?
  - How often is training conducted?
- Does IT conduct audits of "EDL" usage for volume and access beyond the "need to know"?

Policy Considerations

- Are employees prohibited from storing intellectual property (IP) at home?
- Can an employee use home computers to back-up IP prior to traveling overseas?
- Are employees allowed to use their own thumb or external drives, or must they use company issue?
- Does the company have its new and outgoing employees sign non-disclosure agreements?

Foreign Travel Considerations

- Where is your laptop's hard drive and thumb drives when you are out to dinner?
- Do you transmit IP through the Internet when overseas?
- Do you engage in "inappropriate" behavior that could cause you to be blackmailed?
- Do you have conversations about IP overseas in "unsecured" places or on the phone?
- Ensure export information does not go on trip?
- Pre and post trip briefing and debriefing?

Traveling Overseas

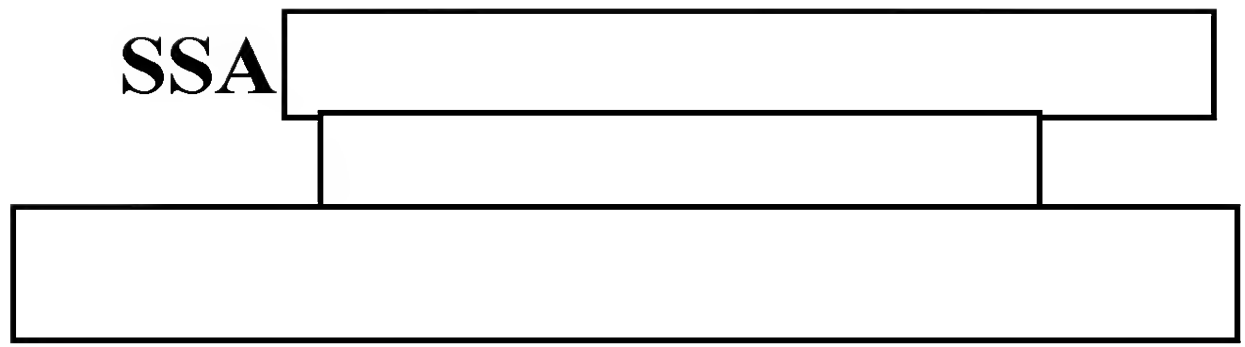
- In most countries, you have no expectation of privacy in Internet cafes, hotels, offices or public places. Hotel business centers and phone networks are regularly monitored in many countries.

- In some countries, hotel rooms are often searched and digital storage devices are copied.

- All information you send electronically can be intercepted.

- Security services and criminals can also insert malicious software into your device through any connection they control.

Questions?



b6
b7C